FIG. 1

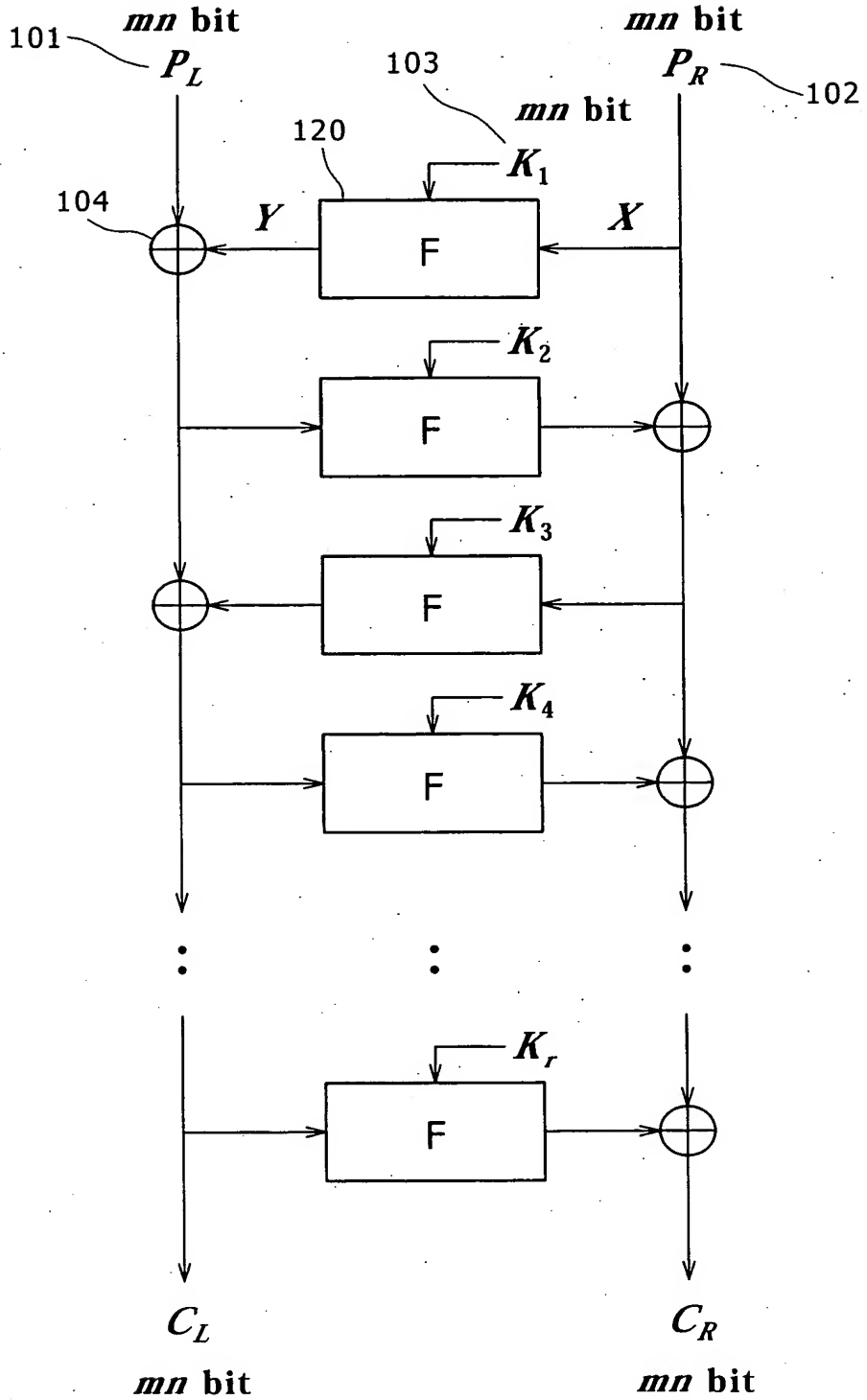

101
mn bit
P_L
103
mn bit
P_R
102
120
K_1
104
Y
X
F
K_2
F
K_3
F
K_4
F
K_r
F
C_L
mn bit
C_R
mn bit

FIG. 2A

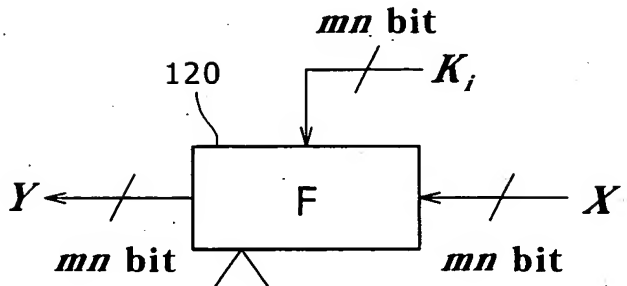

mn bit
K_i
120
F
Y
X
mn bit
mn bit

FIG. 2B

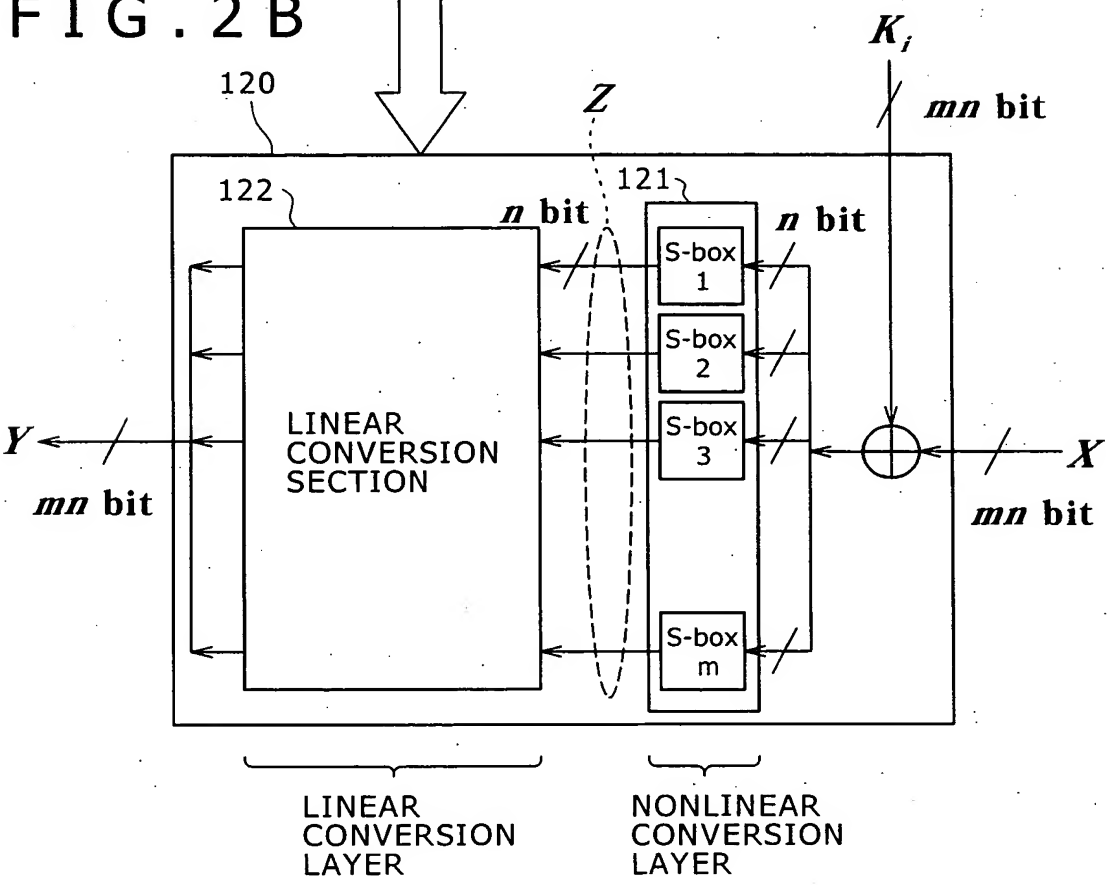

K_i
mn bit
120
Z
122
121
n bit
n bit
S-box 1
S-box 2
S-box 3
S-box m
LINEAR CONVERSION SECTION
Y
mn bit
X
mn bit
LINEAR CONVERSION LAYER
NONLINEAR CONVERSION LAYER

FIG. 3

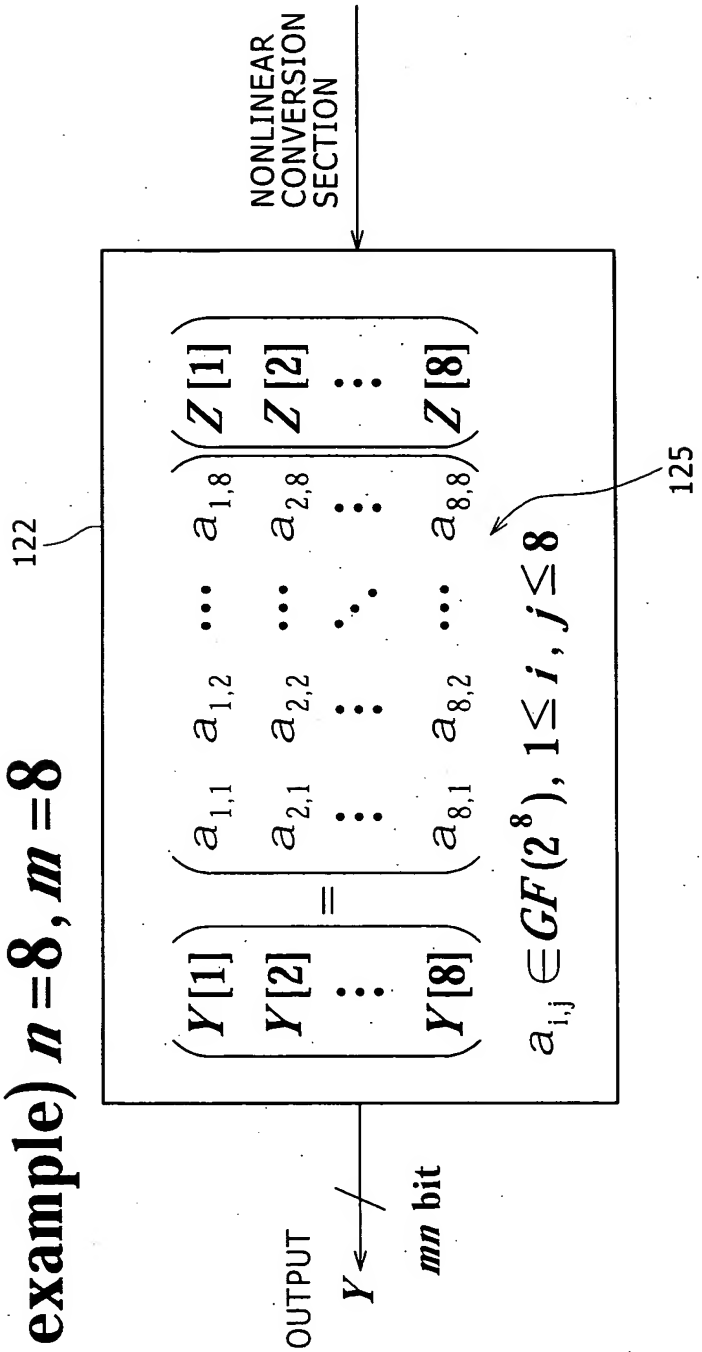

example) $n=8, m=8$
122
NONLINEAR CONVERSION SECTION
$\begin{pmatrix} Y[1] \\ Y[2] \\ \vdots \\ Y[8] \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,8} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,8} \\ \vdots & \vdots & \ddots & \vdots \\ a_{8,1} & a_{8,2} & \cdots & a_{8,8} \end{pmatrix} \begin{pmatrix} Z[1] \\ Z[2] \\ \vdots \\ Z[8] \end{pmatrix}$
$a_{i,j} \in GF(2^8),\ 1 \le i, j \le 8$
125
OUTPUT
Y
mn bit

FIG. 4

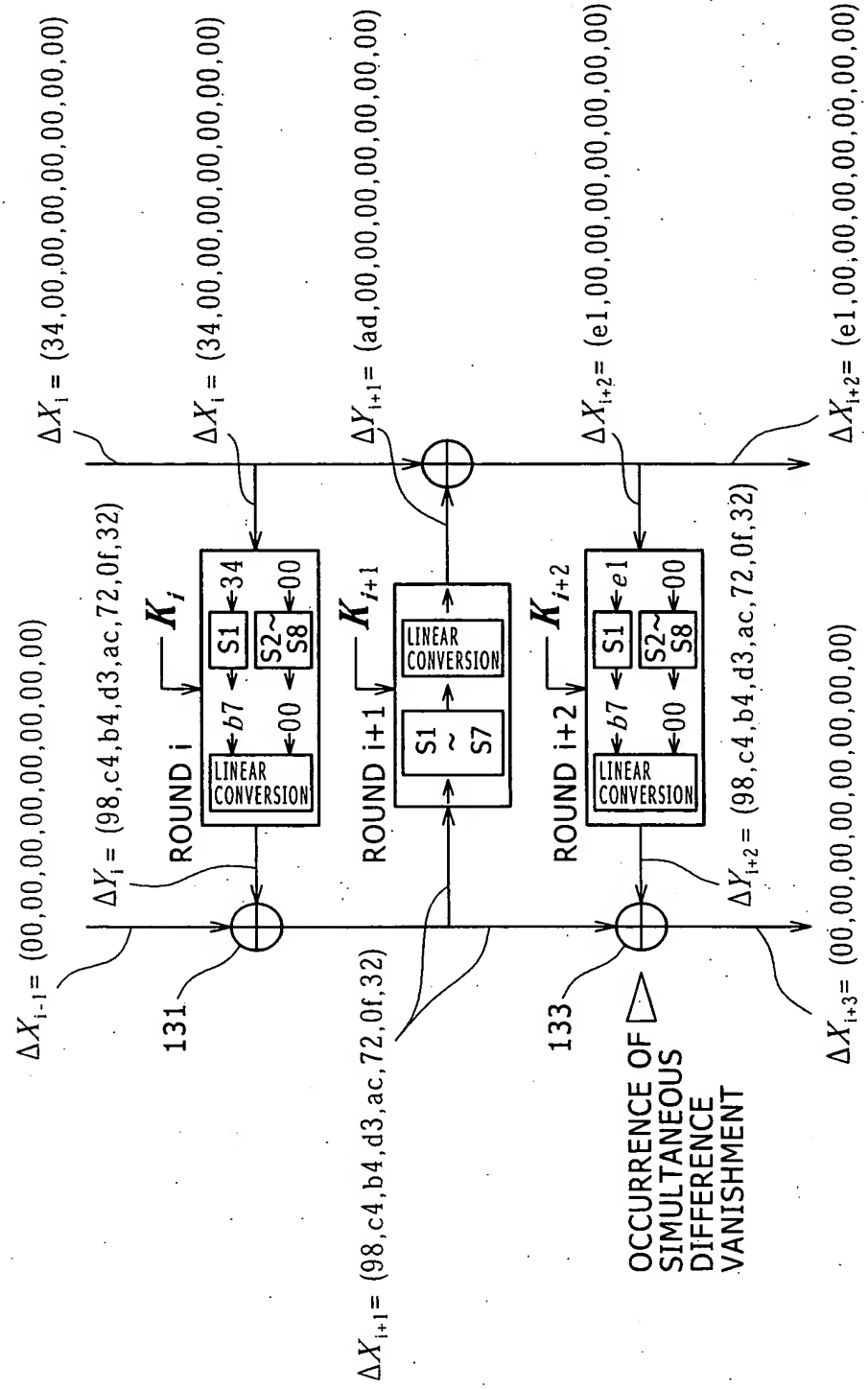

ΔX_i = (34,00,00,00,00,00,00,00)
ΔX_i = (34,00,00,00,00,00,00,00)
ΔY_{i+1} = (ad,00,00,00,00,00,00,00)
ΔX_{i+2} = (e1,00,00,00,00,00,00,00)
ΔX_{i+2} = (e1,00,00,00,00,00,00,00)
ΔY_i = (98,c4,b4,d3,ac,72,0f,32)
ΔX_{i-1} = (00,00,00,00,00,00,00,00)
ROUND i
ROUND i+1
ROUND i+2
K_i
K_{i+1}
K_{i+2}
S1
S2~S8
S1~S7
LINEAR CONVERSION
131
133
ΔX_{i+1} = (98,c4,b4,d3,ac,72,0f,32)
ΔY_{i+2} = (98,c4,b4,d3,ac,72,0f,32)
ΔX_{i+3} = (00,00,00,00,00,00,00,00)
OCCURRENCE OF SIMULTANEOUS DIFFERENCE VANISHMENT

FIG. 5

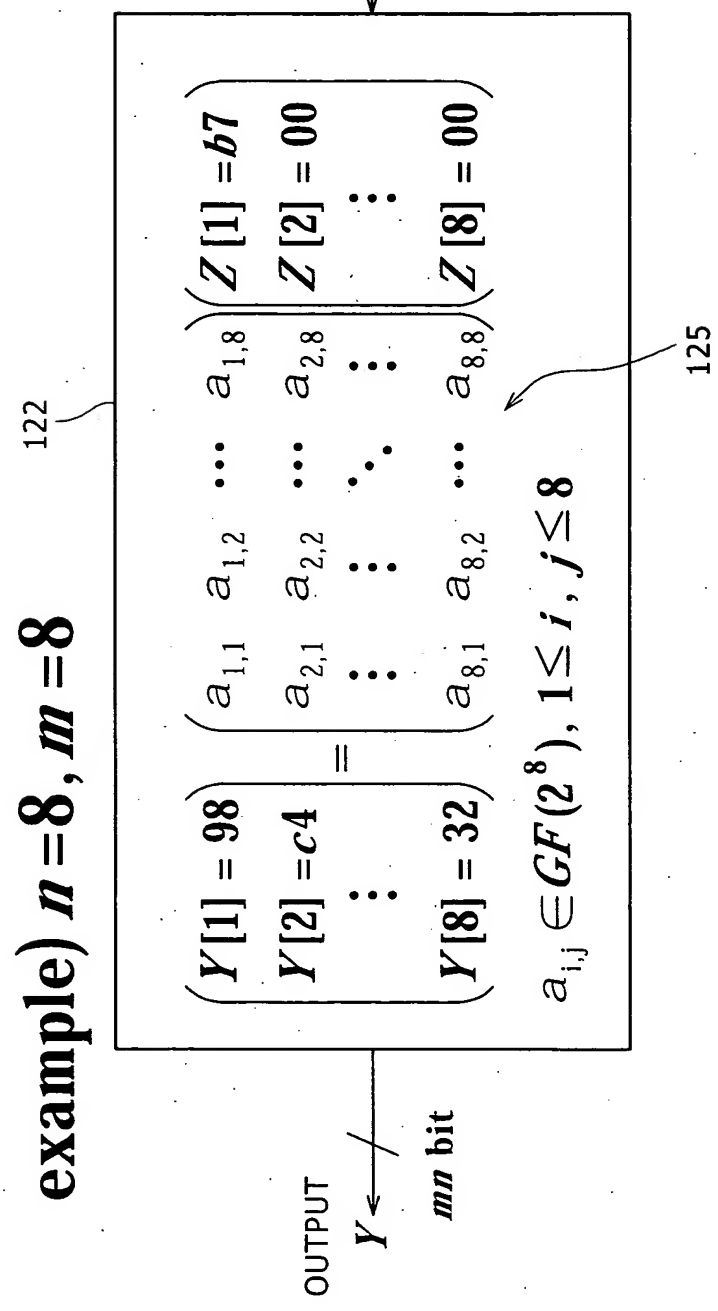

example) $n=8, m=8$
122
NONLINEAR CONVERSION SECTION
$\begin{pmatrix} Y[1]=98 \\ Y[2]=c4 \\ \vdots \\ Y[8]=32 \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,8} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,8} \\ \vdots & \vdots & \ddots & \vdots \\ a_{8,1} & a_{8,2} & \cdots & a_{8,8} \end{pmatrix} \begin{pmatrix} Z[1]=b7 \\ Z[2]=00 \\ \vdots \\ Z[8]=00 \end{pmatrix}$
$a_{i,j} \in GF(2^8),\ 1 \le i, j \le 8$
125
OUTPUT
Y
mn bit

FIG. 6

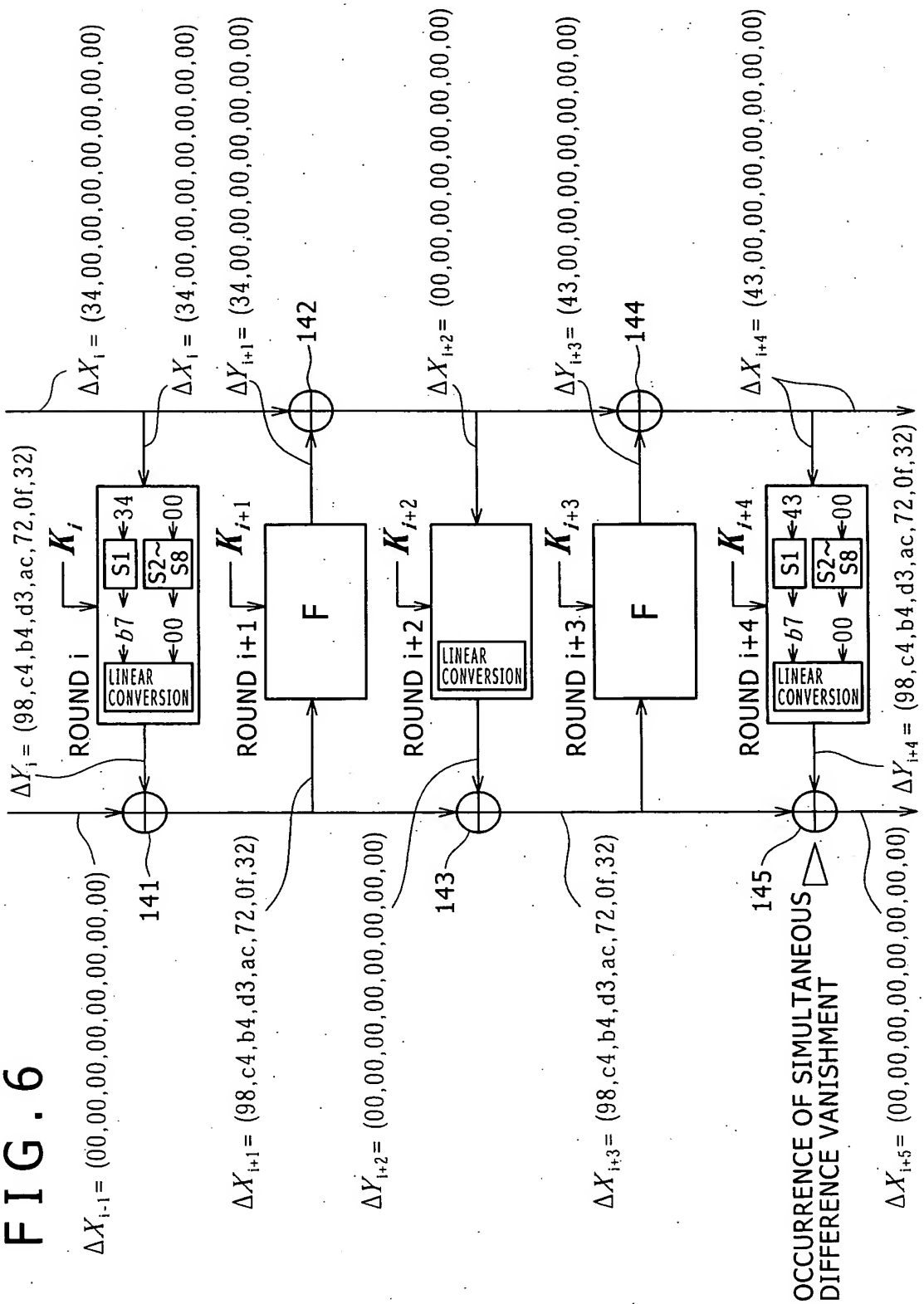

ΔX_{i-1} = (00,00,00,00,00,00,00,00)
ΔY_i = (98,c4,b4,d3,ac,72,0f,32)
ΔX_i = (34,00,00,00,00,00,00,00)
ROUND i
K_i
S1
34
S2~S8
00
b7
00
LINEAR CONVERSION
141
ΔX_{i+1} = (98,c4,b4,d3,ac,72,0f,32)
ΔY_{i+1} = (34,00,00,00,00,00,00,00)
ROUND i+1
K_{i+1}
F
142
ΔX_{i+2} = (00,00,00,00,00,00,00,00)
ΔY_{i+2} = (00,00,00,00,00,00,00,00)
ROUND i+2
K_{i+2}
LINEAR CONVERSION
143
ΔX_{i+3} = (98,c4,b4,d3,ac,72,0f,32)
ΔY_{i+3} = (43,00,00,00,00,00,00,00)
ROUND i+3
K_{i+3}
F
144
ΔX_{i+4} = (43,00,00,00,00,00,00,00)
ΔY_{i+4} = (98,c4,b4,d3,ac,72,0f,32)
ROUND i+4
K_{i+4}
S1
43
S2~S8
00
b7
00
LINEAR CONVERSION
145
OCCURRENCE OF SIMULTANEOUS DIFFERENCE VANISHMENT
ΔX_{i+5} = (00,00,00,00,00,00,00,00)

FIG. 7

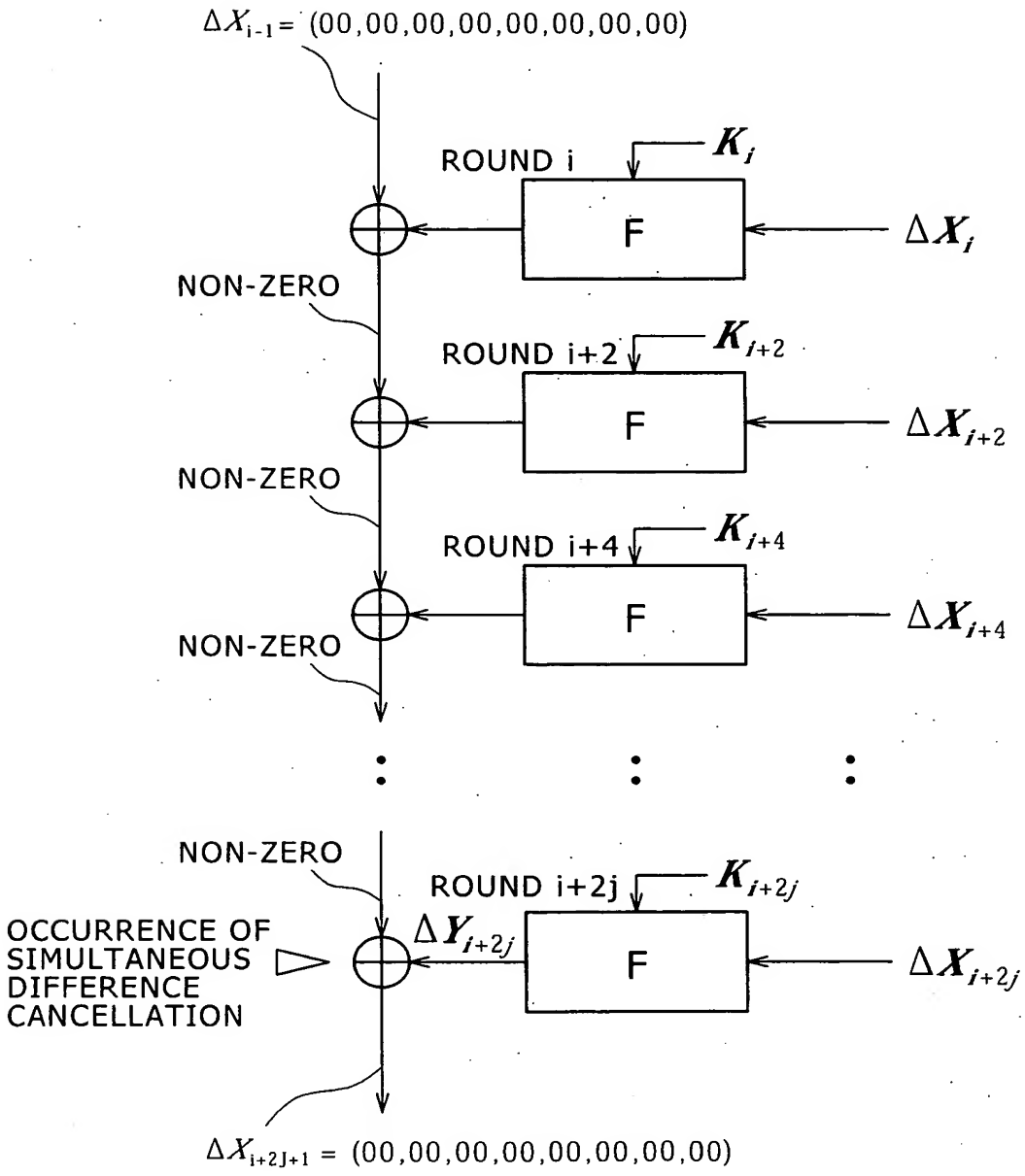

ΔX i-1 = (00,00,00,00,00,00,00,00)
ROUND i
Ki
F
ΔXi
NON-ZERO
ROUND i+2
Ki+2
F
ΔXi+2
NON-ZERO
ROUND i+4
Ki+4
F
ΔXi+4
NON-ZERO
NON-ZERO
ROUND i+2j
Ki+2j
ΔYi+2j
F
ΔXi+2j
OCCURRENCE OF SIMULTANEOUS DIFFERENCE CANCELLATION
ΔX i+2J+1 = (00,00,00,00,00,00,00,00)

FIG. 8

example) $n=8, m=8$

$$\begin{pmatrix} 9d & b4 & d3 & 5d & 84 & ae & ec & b9 \\ 29 & 34 & 39 & 60 & 5c & 81 & 25 & 13 \\ 67 & 6a & d2 & e3 & 4b & db & 9d & 4 \\ 8e & d7 & e6 & 1b & 8b & 9e & 3a & 91 \\ d9 & e5 & 4d & dd & c6 & 5 & f0 & ad \\ 2a & f7 & 67 & 72 & b1 & 7 & f2 & 27 \\ 42 & e6 & a0 & 4 & f1 & 4 & 7d & 8c \\ 55 & 63 & fa & 51 & c & d9 & 28 & d6 \end{pmatrix}$$

FIG. 9

SETUP EXAMPLE OF r=6 AND q=3

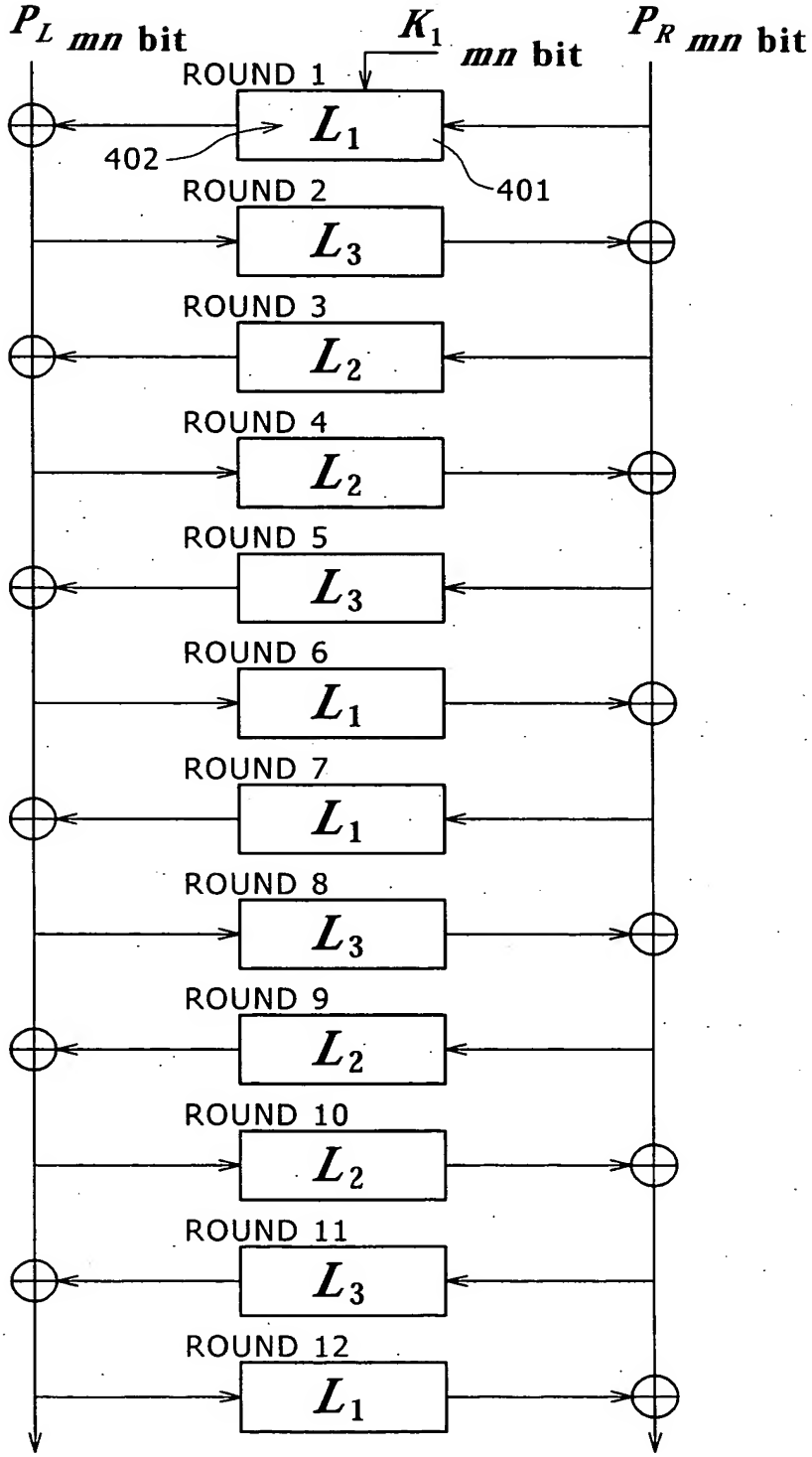


FIG. 10

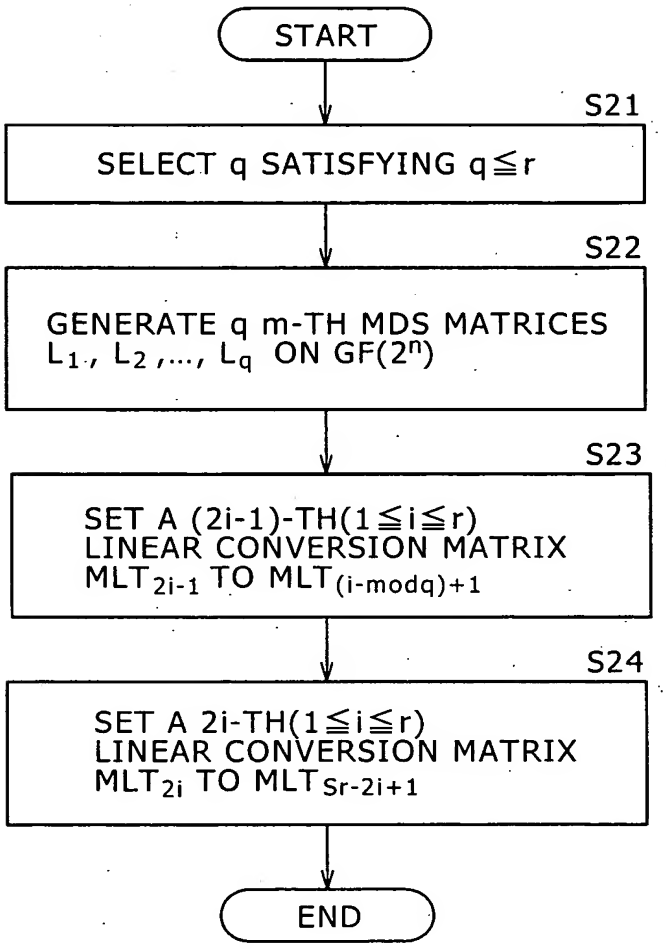

START
S21
SELECT q SATISFYING q≦r
S22
GENERATE q m-TH MDS MATRICES
$L_1, L_2, \ldots, L_q$ ON GF(2^n)
S23
SET A (2i-1)-TH($1 \leqq i \leqq r$)
LINEAR CONVERSION MATRIX
MLT_{2i-1} TO $MLT_{(i-modq)+1}$
S24
SET A 2i-TH($1 \leqq i \leqq r$)
LINEAR CONVERSION MATRIX
MLT_{2i} TO $MLT_{Sr-2i+1}$
END

FIG. 11

CASE OF q=6, n=8, AND m=8

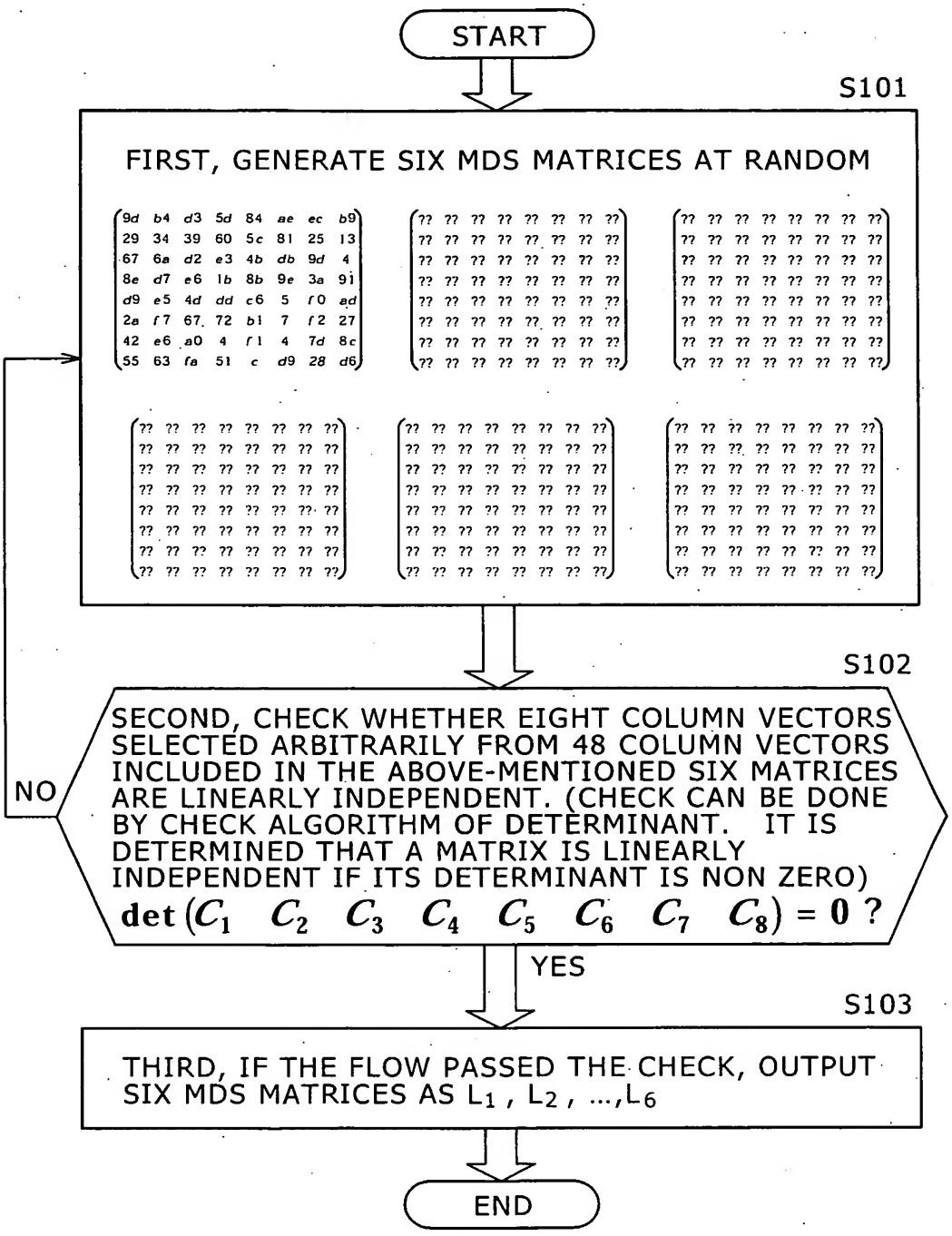


FIG. 12

CASE OF q=6, n=8, AND m=8

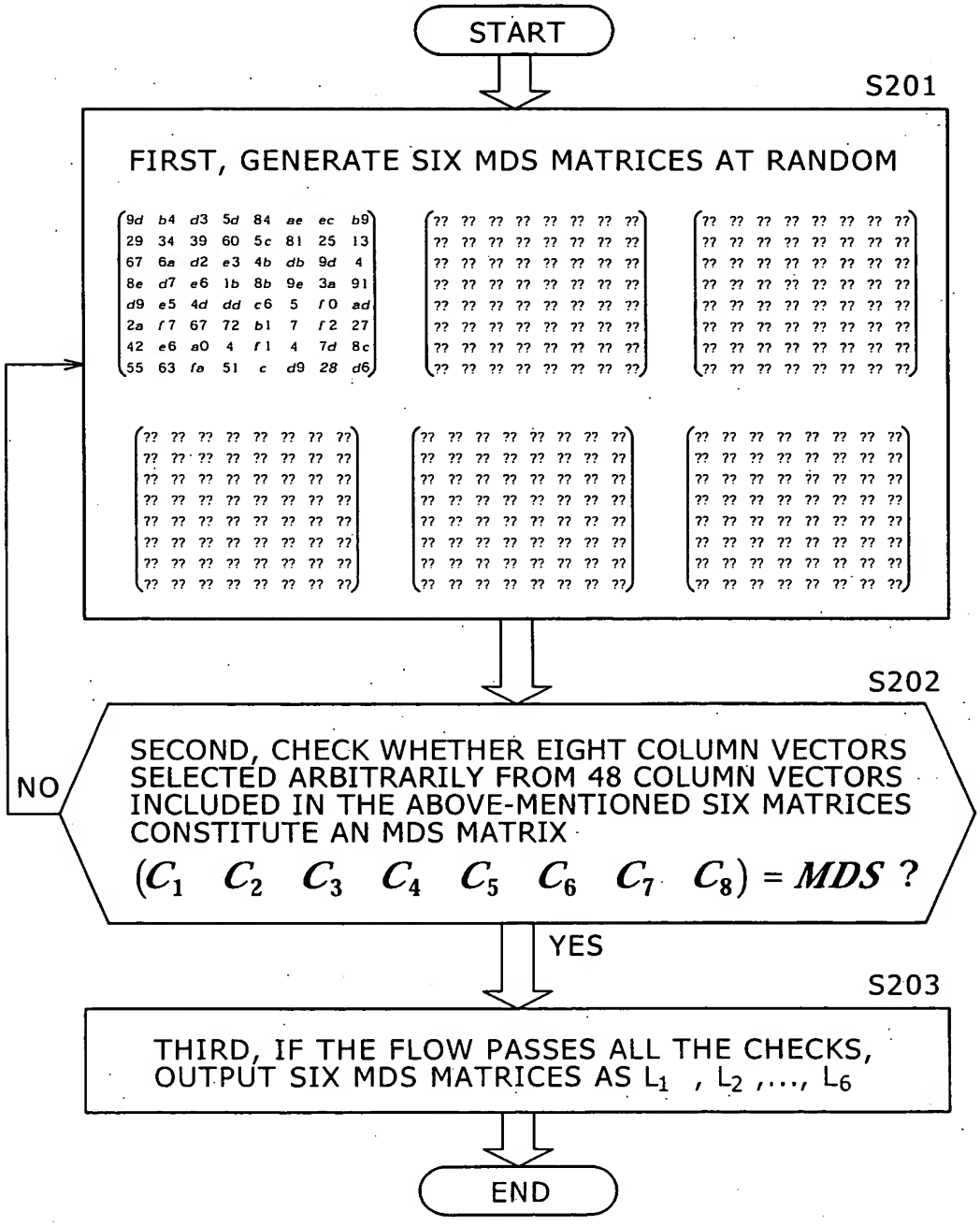


FIG. 13

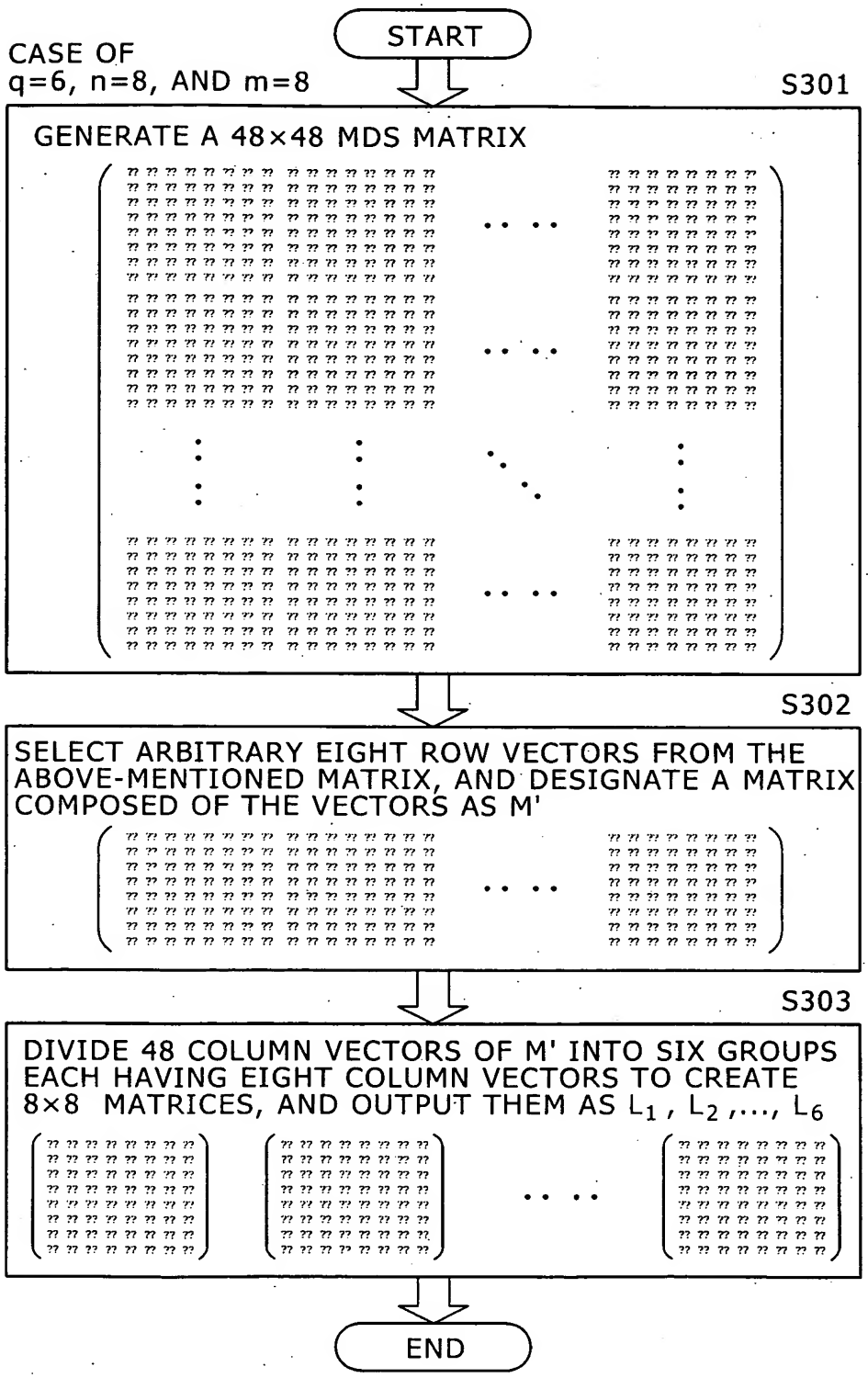

START
CASE OF
q=6, n=8, AND m=8
S301
GENERATE A 48×48 MDS MATRIX
S302
SELECT ARBITRARY EIGHT ROW VECTORS FROM THE ABOVE-MENTIONED MATRIX, AND DESIGNATE A MATRIX COMPOSED OF THE VECTORS AS M'
S303
DIVIDE 48 COLUMN VECTORS OF M' INTO SIX GROUPS EACH HAVING EIGHT COLUMN VECTORS TO CREATE 8×8 MATRICES, AND OUTPUT THEM AS L1 , L2 ,..., L6
END

FIG. 14

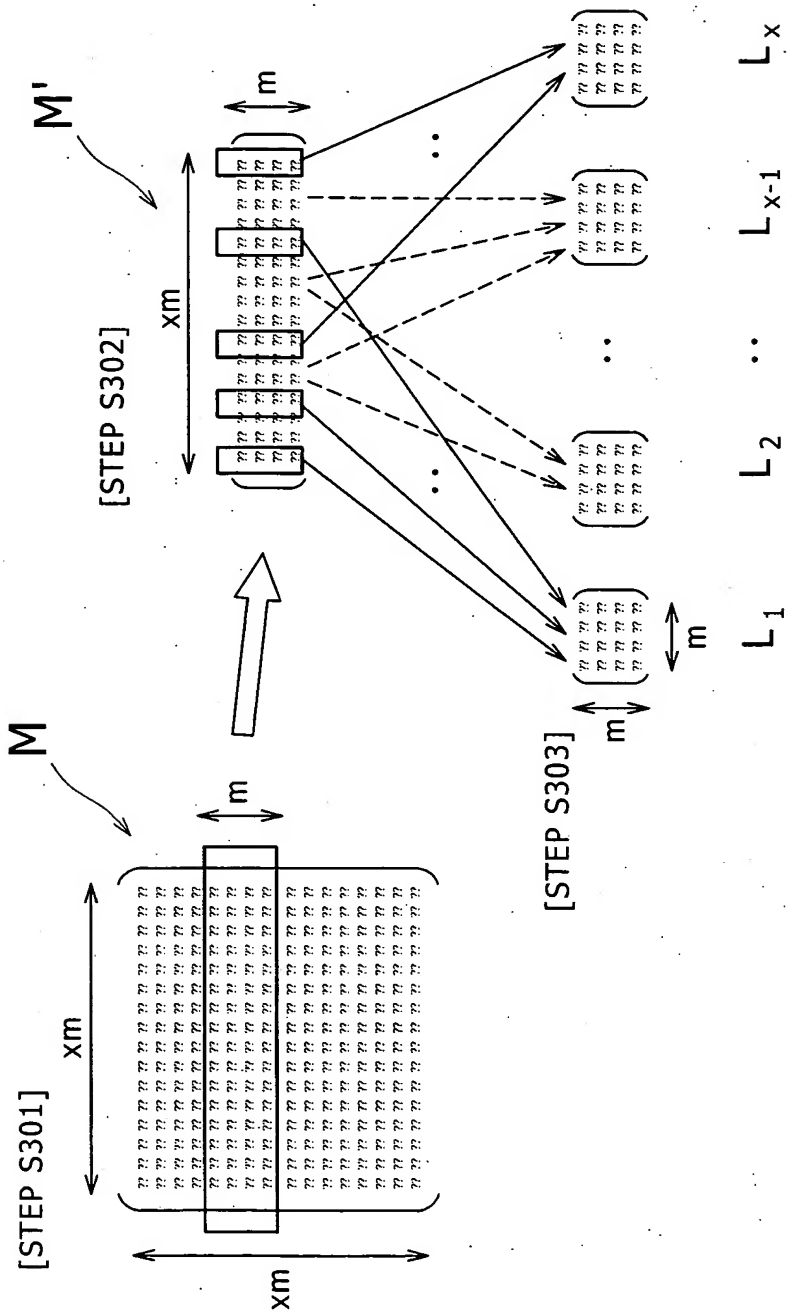


FIG. 15

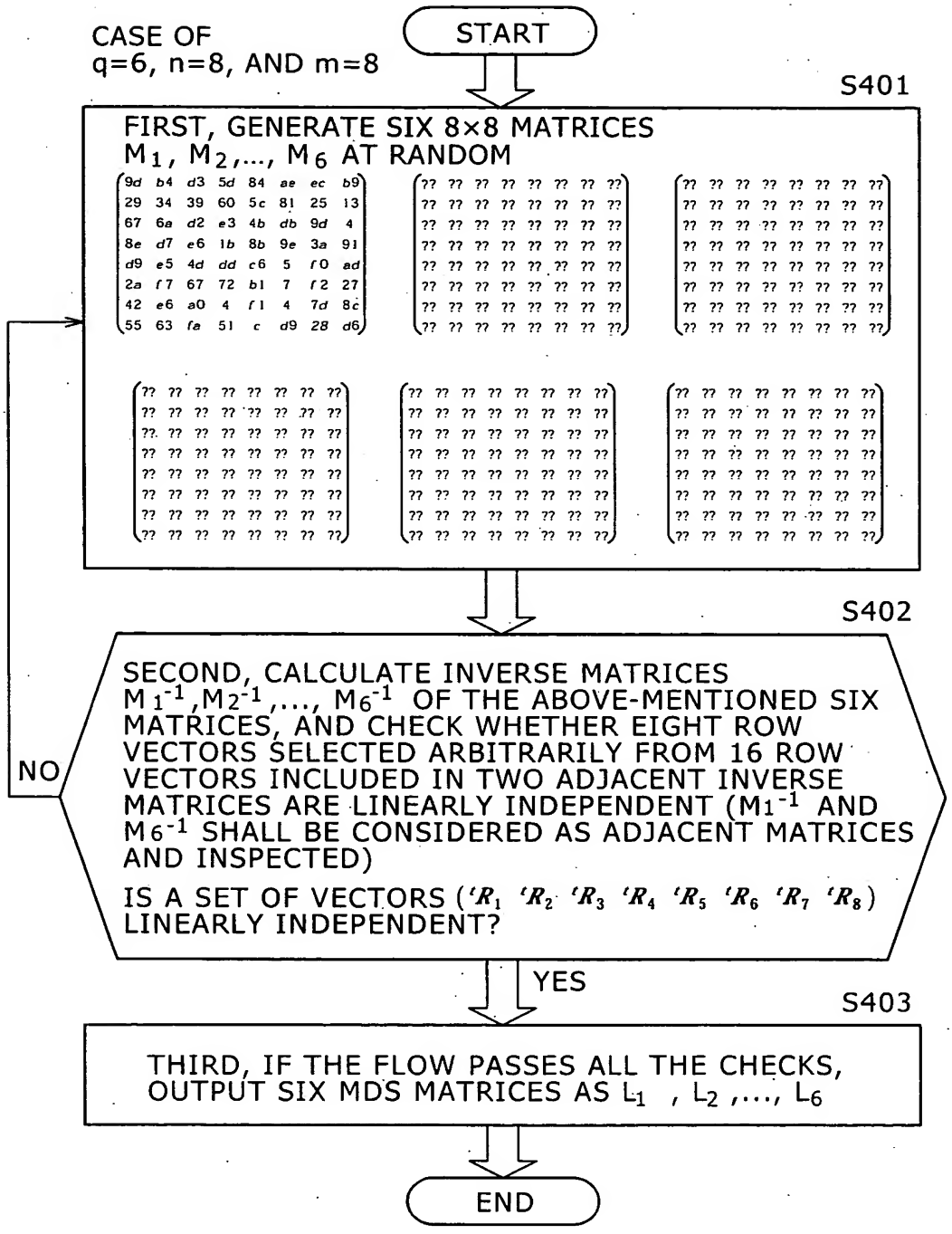

CASE OF
q=6, n=8, AND m=8
START
S401
FIRST, GENERATE SIX 8×8 MATRICES
M1, M2,..., M6 AT RANDOM
9d b4 d3 5d 84 ae ec b9
29 34 39 60 5c 81 25 13
67 6a d2 e3 4b db 9d 4
8e d7 e6 1b 8b 9e 3a 91
d9 e5 4d dd c6 5 f0 ad
2a f7 67 72 b1 7 f2 27
42 e6 a0 4 f1 4 7d 8c
55 63 fa 51 c d9 28 d6
S402
SECOND, CALCULATE INVERSE MATRICES M1-1,M2-1,..., M6-1 OF THE ABOVE-MENTIONED SIX MATRICES, AND CHECK WHETHER EIGHT ROW VECTORS SELECTED ARBITRARILY FROM 16 ROW VECTORS INCLUDED IN TWO ADJACENT INVERSE MATRICES ARE LINEARLY INDEPENDENT (M1-1 AND M6-1 SHALL BE CONSIDERED AS ADJACENT MATRICES AND INSPECTED)
IS A SET OF VECTORS ('R1 'R2 'R3 'R4 'R5 'R6 'R7 'R8) LINEARLY INDEPENDENT?
NO
YES
S403
THIRD, IF THE FLOW PASSES ALL THE CHECKS, OUTPUT SIX MDS MATRICES AS L1 , L2 ,..., L6
END

FIG. 16

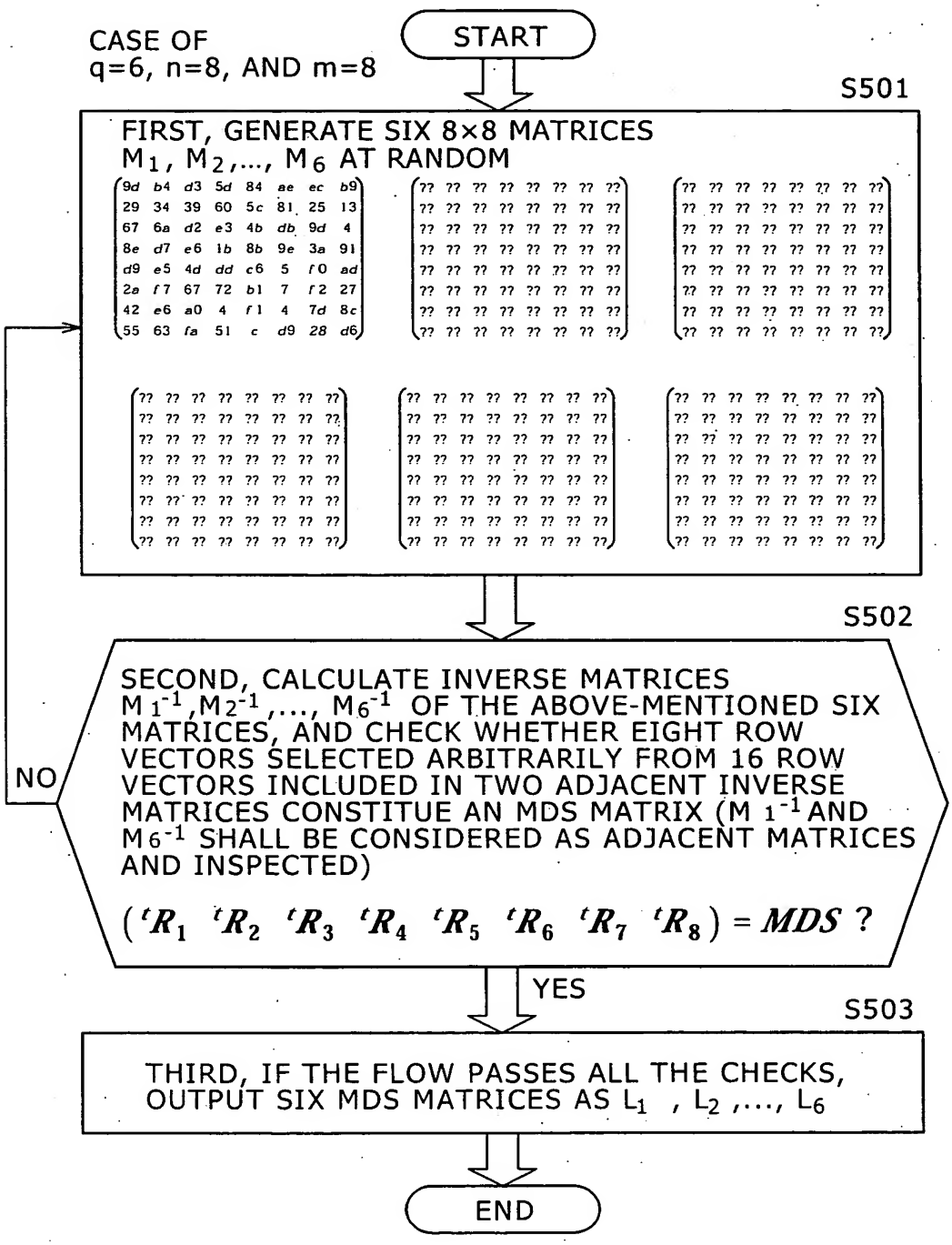

CASE OF
q=6, n=8, AND m=8
START
S501
FIRST, GENERATE SIX 8×8 MATRICES
M1, M2,..., M6 AT RANDOM
9d b4 d3 5d 84 ae ec b9
29 34 39 60 5c 81 25 13
67 6a d2 e3 4b db 9d 4
8e d7 e6 1b 8b 9e 3a 91
d9 e5 4d dd c6 5 f0 ad
2a f7 67 72 b1 7 f2 27
42 e6 a0 4 f1 4 7d 8c
55 63 fa 51 c d9 28 d6
S502
SECOND, CALCULATE INVERSE MATRICES M1-1,M2-1,..., M6-1 OF THE ABOVE-MENTIONED SIX MATRICES, AND CHECK WHETHER EIGHT ROW VECTORS SELECTED ARBITRARILY FROM 16 ROW VECTORS INCLUDED IN TWO ADJACENT INVERSE MATRICES CONSTITUE AN MDS MATRIX (M 1-1 AND M6-1 SHALL BE CONSIDERED AS ADJACENT MATRICES AND INSPECTED)
(tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) = MDS ?
NO
YES
S503
THIRD, IF THE FLOW PASSES ALL THE CHECKS, OUTPUT SIX MDS MATRICES AS L1 , L2 ,..., L6
END

FIG. 17

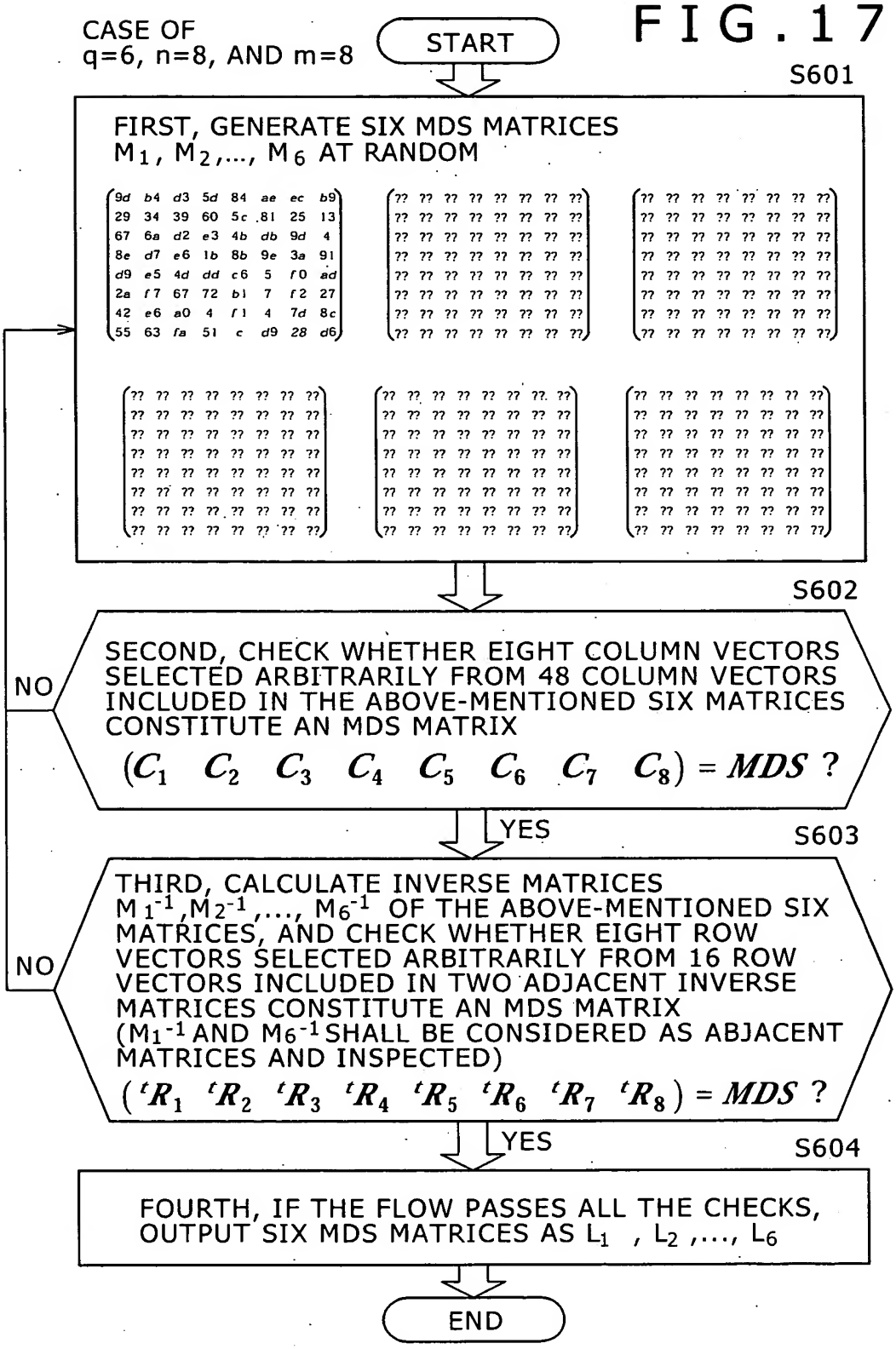
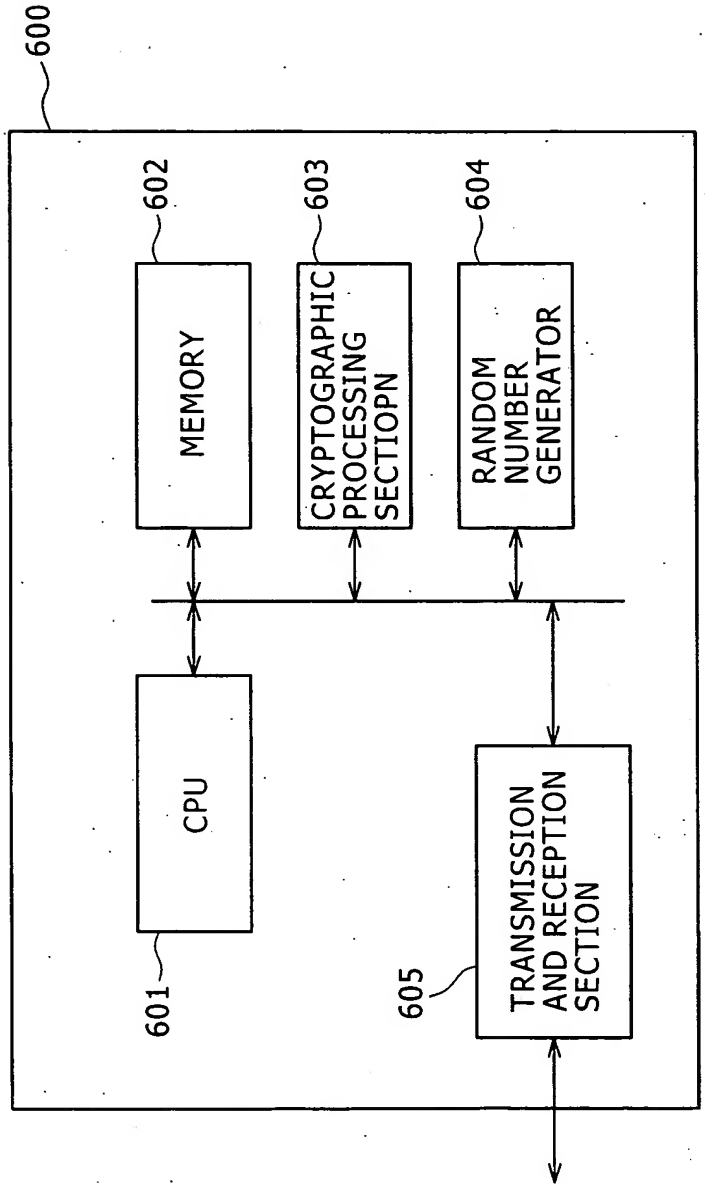

CASE OF
q=6, n=8, AND m=8
START
S601
FIRST, GENERATE SIX MDS MATRICES
M1, M2,..., M6 AT RANDOM
S602
SECOND, CHECK WHETHER EIGHT COLUMN VECTORS SELECTED ARBITRARILY FROM 48 COLUMN VECTORS INCLUDED IN THE ABOVE-MENTIONED SIX MATRICES CONSTITUTE AN MDS MATRIX
(C1 C2 C3 C4 C5 C6 C7 C8) = MDS ?
NO
YES
S603
THIRD, CALCULATE INVERSE MATRICES M1-1, M2-1,..., M6-1 OF THE ABOVE-MENTIONED SIX MATRICES, AND CHECK WHETHER EIGHT ROW VECTORS SELECTED ARBITRARILY FROM 16 ROW VECTORS INCLUDED IN TWO ADJACENT INVERSE MATRICES CONSTITUTE AN MDS MATRIX
(M1-1 AND M6-1 SHALL BE CONSIDERED AS ABJACENT MATRICES AND INSPECTED)
(tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) = MDS ?
NO
YES
S604
FOURTH, IF THE FLOW PASSES ALL THE CHECKS, OUTPUT SIX MDS MATRICES AS L1 , L2 ,..., L6
END

FIG.18


600
602
603
604
MEMORY
CRYPTOGRAPHIC PROCESSING SECTIOPN
RANDOM NUMBER GENERATOR
CPU
TRANSMISSION AND RECEPTION SECTION
601
605